METHOD FOR REGULATING AND MANAGING USE OF VIRTUAL PRIVATE NETWORK AND ITS SYSTEM

Patent Number: JP2001251307

Publication date: 2001-09-14

Inventor(s): MIYOSHI JUN;; IMAIDA ISAMUNE;; KANEKO

Applicant(s): NIPPON TELEGR & TELEPH CORP

Requested Patent: ⌜ JP2001251307

Application Priority Number(s): JP20000057568 20000302

IPC Classification: H04L12/28; H04L12/56

EC Classification:

Equivalents:

Abstract

PROBLEM TO BE SOLVED: To provide a method for regulating and managing use of a virtual private network and its system that can reduce a load of a broadband IP network and a VPN manager and operate an element control function on the basis of VPN utilization regulations.
SOLUTION: A policy storage section 13 stores a policy of a broadband IP network and a policy of a VPN, a policy verification function section 12 verifies a contradiction between the policy of the broadband IP network and a registration request of the policy of the VPN and a contradiction between regulations of use of the registered virtual private network and a service request from an end user, and the VPN policy is registered or set to a QoS controller 5 and a security controller 6 via a common platform section 14, a QoS policy control section 15 and a security policy control section 16 according to the result of verification.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－251307
（P2001－251307A）
(43)公開日　平成13年９月14日(2001.9.14)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｈ０４Ｌ　12/28		Ｈ０４Ｌ　11/20	Ｇ　５Ｋ０３０
12/56			１０２Ａ　９Ａ００１

審査請求　未請求　請求項の数５　ＯＬ　（全 10 頁）

(21)出願番号　特願2000－57568(P2000－57568)

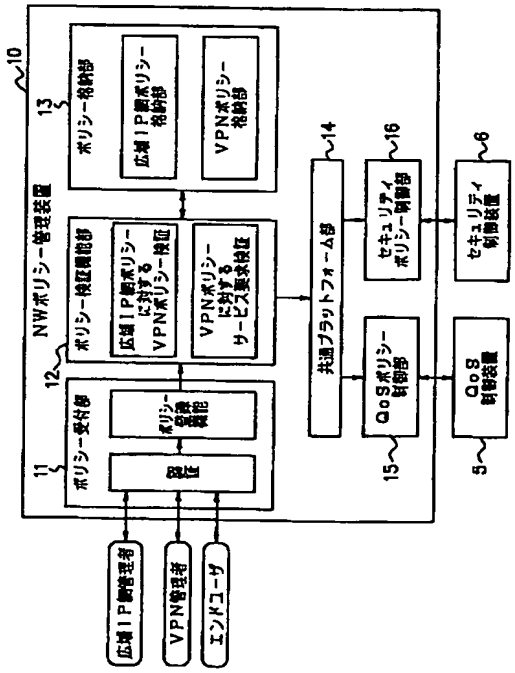
(22)出願日　平成12年３月２日(2000.3.2)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　三好　潤
東京都千代田区大手町２丁目３番１号　日本電信電話株式会社内
(72)発明者　今井田　伊佐宗
東京都千代田区大手町２丁目３番１号　日本電信電話株式会社内
(74)代理人　100069981
弁理士　吉田　精孝

最終頁に続く

(54)【発明の名称】　仮想プライベートネットワーク利用規定管理方法及びその装置

(57)【要約】
【課題】　広域ＩＰ網及びＶＰＮ管理者の負担を軽減し、ＶＰＮの利用規定に基づいてエレメント制御機能を運用できる仮想プライベートネットワーク利用規定管理方法及びその装置を提供すること。
【解決手段】　ポリシー格納部１３に広域ＩＰ網のポリシー及びＶＰＮのポリシーを格納しておき、広域ＩＰ網のポリシーとＶＰＮ管理者からのＶＰＮのポリシーの登録要求との矛盾や登録済の仮想プライベートネットワークの利用規定とエンドユーザからのサービス要求との矛盾をポリシー検証機能部１２にて検証し、検証結果に従ってＶＰＮポリシーを登録し、あるいは共通プラットフォーム部１４、ＱｏＳポリシー制御部１５及びセキュリティポリシー制御部１６を介してＱｏＳ制御装置５及びセキュリティ制御装置６を設定する。



【特許請求の範囲】
【請求項１】　広域ＩＰ網上に構築され、運用される仮想プライベートネットワークにおける利用規定の管理方法であって、
複数の仮想プライベートネットワーク毎に定める利用規定の管理を行い、
仮想プライベートネットワーク間通信時のエンドユーザからのサービス要求を、要求元の仮想プライベートネットワークの利用規定と、通信相手先の仮想プライベートネットワークの利用規定との双方で検証することを特徴とする仮想プライベートネットワーク利用規定管理方法。
【請求項２】　仮想プライベートネットワークの利用規定を、広域ＩＰ網の管理者と、少なくとも１つの仮想プライベートネットワークの管理権限を持つ管理者とで階層的に管理することを特徴とする請求項１記載の仮想プライベートネットワーク利用規定管理方法。
【請求項３】　単一の仮想プライベートネットワークの管理権限を持つ管理者が複数の仮想プライベートネットワークを管理する場合、これらの仮想プライベートネットワーク間通信に関する仮想プライベートネットワークの利用規定を自動生成することを特徴とする請求項１記載の仮想プライベートネットワーク利用規定管理方法。
【請求項４】　エンドユーザからのサービス要求を、帯域保証制御や仮想プライベートネットワーク間接続に必要なセキュリティ制御等を行う各ネットワーク構成装置の制御装置の設定情報に変換して配信することを特徴とする請求項１記載の仮想プライベートネットワーク利用規定管理方法。
【請求項５】　広域ＩＰ網上に構築され、運用される仮想プライベートネットワークにおける利用規定の管理装置であって、
広域ＩＰ網の利用規定及び仮想プライベートネットワークの利用規定を格納する格納部と、
広域ＩＰ網の利用規定と仮想プライベートネットワークの利用規程との矛盾や登録済の仮想プライベートネットワークの利用規定とエンドユーザからのサービス要求との矛盾を検証する検証機能部と、
仮想プライベートネットワークの管理者からの利用規程の登録要求を受け付け、広域ＩＰ網の利用規定との検証結果に従って格納部に格納するとともに、エンドユーザからのサービス要求を受け付ける受付部と、
サービス要求の検証結果に従ってネットワーク構成装置の帯域保証制御装置及びセキュリティ制御装置に対する設定を行う制御部とを備えたことを特徴とする仮想プライベートネットワーク利用規定管理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、広域ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）網上に構築され、運用される仮想プライベートネットワークにおける利用規定の管理方法及びその装置に関するものである。
【０００２】
【従来の技術】ネットワーク（以下、NWと略記する。）における利用規程（以下、ポリシーと呼ぶ。）の管理技術については、情報処理学会シンポジウム論文集、ｖｏｌ．９８、Ｎｏ．８、ｐ４１－４８等において既知の技術として公開されており、また、ＩＥＴＦ（Ｔｈｅ　Ｉｎｔｅｒｎｅｔ　Ｅｎｇｉｎｅｅｒｉｎｇ　ＴａｓｋＦｏｒｃｅ）のＰｏｌｉｃｙ　Ｆｒａｍｅｗｏｒｋ　ワーキンググループ（以下、ｐｏｌｉｃｙ　WGと略記する。）等においてもポリシー管理技術に関する提案がなされている。
【０００３】しかし、これらの技術を用いた既存のNWポリシー管理装置はユーザNWに閉じた範囲を想定したものであり、ポリシー管理者及びエンドユーザという二層の管理構造しか持っておらず、また、仮想的なプライベートネットワーク（以下、ＶＰＮと略記する。）を跨ったポリシーの管理は実現できていない。そのため、第１種及び第２種通信事業者等（以下、キャリアと呼ぶ。）が提供し、複数ユーザがリソースを共有する、ＩＰ　ｏｖｅｒ　ＦＲ（Ｆｒａｍｅ　Ｒｅｌａｙ）やＩＰ　ｏｖｅｒ　ＡＴＭ等の広域ＩＰ網上にＶＰＮが構築され、運用される場合、ＶＰＮ間でポリシーの競合が発生する可能性があり、対応が困難であった。
【０００４】従来、広域ＩＰ網は全て広域ＩＰ網管理者が管理していたため、エンドユーザからのサービス要求はユーザ側のＶＰＮ管理者が仲介する形で、広域ＩＰ網管理者へ申し込みを行う必要があった。そのため、サービス要求発生から実際にサービス変更が行われるまでのタイムラグが大きく、仲介する要員の稼働が大きくなるという問題があった。
【０００５】従来の広域ＩＰ網上のＶＰＮに対するサービス変更の流れの概略を図１に示す。
【０００６】運用中のNWについてのサービス要求はエンドユーザから発生する。具体的にはＶＰＮ間のフィルタリング解除要求や、帯域保証（またはサービス品質）（以下、ＱｏＳと略記する。）要求等である。ＶＰＮ管理者は、これらのサービス要求を受け付け（Ｓ１）、自NWの利用規定に基づいてその要求に対する可否判断を行う（Ｓ２）。自NW内の構成装置（エレメント）に対してのみ変更の場合は自NW内で完結する（Ｓ３）が、広域ＩＰ網を跨る設定の場合はサービスを提供する広域ＩＰ網管理者へ依頼する必要がある（Ｓ４）。
【０００７】要求を受け取った広域ＩＰ網管理者（Ｓ５）は、広域ＩＰ網の利用規定に基づいてその要求に対する可否判断を行った（Ｓ６）後、必要ならサービス要求を実施し（Ｓ７）、完了報告を行う（Ｓ８）。完了報告を受けたＶＰＮ管理者はサービス要求を発生したエンドユーザに完了報告を行う（Ｓ９）。

【0008】
【発明が解決しようとする課題】このように、従来のNWポリシー管理装置では、VPN間相互接続の際、VPN間通信に双方のVPNポリシーを反映させることが困難であり、複数のVPN間でVPNポリシーの競合が発生する。このため、広域IP網管理者及びVPN管理者の調整稼動が大きくなり、VPNの運用形態の変化に柔軟に対応することが困難であった。よって管理負担を軽減し、管理者のポリシーに基づいてNWを効率的に制御することが目的のNWポリシー管理装置を導入しても、効果が得られないという問題があった。
【0009】さらにサービス要求に対して、QoSやセキュリティ等の各エレメント制御機能を連携して制御する機能を有しておらず、それぞれのエレメントを制御するNWポリシー管理装置毎にポリシー設定及びサービス要求を行う必要があり、ポリシー設定に矛盾が発生する恐れのあることも問題であった。
【0010】本発明の目的は、広域IP網管理者及びVPN管理者の管理負担を軽減し、VPN管理者が規定したVPNポリシーに基づいてQoSやセキュリティ等のエレメント制御機能を運用できる、仮想プライベートネットワーク利用規定（VPNポリシー）管理方法及びその装置を提供することにある。
【0011】
【課題を解決するための手段】本発明では、前記課題を解決するため、広域IP網を管理するキャリア側の広域IP網管理者は広域IP網全体に関わるNW管理ポリシーを管理し、個々のVPN内のVPNポリシーについてはそれぞれのVPN管理者が管理する。このようにポリシーを階層的に管理することにより、VPN管理者は権限の範囲内でVPNの運用形態に応じた柔軟なVPNポリシーの設定、変更が可能となり、VPN管理者及び広域IP網管理者の管理負担を軽減できる。
【0012】また、VPNを跨るサービス要求が発生した場合は要求元のみならず、通信相手先のVPNポリシーとも照合を行うことにより、双方のVPNポリシーを反映したVPN間通信が可能となる。
【0013】また、単一のVPNの管理権限を持つ管理者が複数のVPNを管理する場合、該管理者が管理権限を持つVPN群をVPNグループとし、VPNグループ内のVPN間通信に関わるVPNポリシーの設定の矛盾を自動的に回避することにより、VPN間通信に関するポリシー設定作業を簡略化することができる。即ち、一方のVPNにおけるVPNポリシーをVPN管理者が設定し、その通信相手先のVPNが同一VPNグループ内であると判断された場合は、通信相手先のVPNにもVPN間通信に関するVPNポリシーを自動生成する。この際、各々のVPNが異なるアドレス体系を持つ場合も、アドレス変換情報を元にVPNポリシーの自動生成を行う。
【0014】さらに、エンドユーザから設定されるQoS及びVPNを跨った通信の要求を、これらのVPNポリシーで検証した後に、QoS制御やVPN間接続に必要なセキュリティ制御等を行う広域IP網における各ネットワークエレメントの制御装置の設定情報に変換して配信する。これにより、広域IP網上でQoSやセキュリティ等のネットワーク機能をポリシーに基づいて連携制御可能とする。
【0015】以上の過程をもって上記課題を解決する。
【0016】
【発明の実施の形態】以下、図面を用いて本発明の実施の形態を説明する。
【0017】図2は本発明の実施の形態の一例を示すもので、複数のユーザ（もしくはユーザNW）1a，1b，1c及び2a，2b，2cがエッジルータ（ER）を介して広域IP網3に接続され、それぞれVPN#1及びVPN#2というWAN（Wide Area Network）を構成するネットワーク全体を示している。
【0018】本発明のVPNポリシー管理装置（以下、PMSと略記する。）10は、エッジルータを介して広域IP網3に接続されており、また、網管理用NW4というLAN（Local Area Network）にも接続されており、これを用いてNWを構成する各装置（エレメント）の制御装置との通信を行う（請求項4）。広域IP網管理者はPMS10のコンソール上において操作を行い、VPN管理者及びエンドユーザはVPN#1，VPN#2経由でPMS10に接続し、設定等の操作を行う。
【0019】NWポリシーを構成する情報はIETFのpolicy WGによって図3に示すように提案されており、本発明では各構成情報の管理者を図4に示すように階層化、即ちキャリア側の広域IP網管理者を広域IP網管理者、ユーザNW側管理者をVPN管理者として位置付け、それぞれのVPNポリシーについて広域IP網管理者は各VPN契約情報の管理を行い、VPN管理者は管理下にあるVPN内の帯域、セキュリティの運用ルールの管理を行うことにより、VPNポリシーの管理権限分散を行う。
【0020】これによって、従来のサービス要求の際に必要とされた、広域IP網管理者とVPN管理者との間での申し込みや受付、エンドユーザとVPN管理者との間での申し込みや受付等、通常ルーチンで繰り返される手間が省かれることになる（請求項2）。
【0021】また、VPN間相互接続の際、VPNを跨るサービス要求が生じた場合、図5に示すように、ユーザが所属するVPNのポリシーだけでなく、通信相手先のVPNのポリシーを参照し（i）、双方で検証されることで、相互のVPNのポリシーに基づくセキュリティの高い通信が可能となる（請求項1）。

【００２２】さらに、図５に示すように、企業内、学校内等で複数のＶＰＮを部署毎、学部毎に契約している場合は複数のＶＰＮをグループ化し、ＶＰＮグループとしてＶＰＮ管理者が複数ＶＰＮに跨るポリシーを扱うことを可能とする。これによりＶＰＮグループ内でのＶＰＮ相互通信についてはＶＰＮグループ内の１ＮＷ管理ポリシーとして登録し、ユーザ要求時にそれを参照する（ｉｉ）ことで検証が行われ、ＶＰＮポリシーの登録と、ＰＭＳ内での検証手順を簡略化できる（請求項２、３）。

【００２３】図６はＰＭＳの構成を示すもので、大きく分けて６つの機能ブロックからなっている。即ち、図中、１１はユーザインタフェースを提供するポリシー受付部、１２は要求された内容を検証するポリシー検証機能部、１３はポリシー情報や操作記録を格納するデータベースのポリシー格納部、１４は制御するネットワークエレメントとのやり取りのための共通プラットフォーム部、１５はネットワークエレメントのＱｏＳを制御するＱｏＳ制御装置５との通信を行うＱｏＳポリシー制御部、１６はネットワークエレメントのセキュリティを制御するセキュリティ制御装置６との通信を行うセキュリティポリシー制御部である。

【００２４】本発明による広域ＩＰ網上のＶＰＮに対するサービス変更に関わる各管理者及びユーザとＰＭＳとのやり取りの概略を図７に示す。

【００２５】また、図８は広域ＩＰ網ポリシー登録時のフローチャートを、図９はＶＰＮポリシー登録時のフローチャートを、図１０はユーザ要求発生時のフローチャートをそれぞれ示すもので、以下、本発明によるサービス変更について説明する。

【００２６】ユーザがポリシーサービスの享受を希望した場合、キャリアである広域ＩＰ網管理者は広域ＩＰ網上においてＶＰＮポリシーサービスのサービスユーザ情報の登録を行う。

【００２７】まず、ＰＭＳ１０のポリシー受付部１１を介してＶＰＮ及びＶＰＮグループの情報を登録し（Ｓ１１）、その管理者情報の登録を行う（Ｓ１２）。その後、サービスの契約条件等に関わる広域ＩＰ網ポリシーを登録し（Ｓ１３）、ポリシー格納部１３に格納する（Ｓ１４）。

【００２８】上記にて登録されたＶＰＮ管理者はポリシー受付部１１を介して自分が管理するユーザＮＷに対してのＶＰＮポリシーのエントリ登録を行う（Ｓ２１）。ＰＭＳ１０ではポリシー検証機能部１２にて広域ＩＰ網ポリシーに照らし合わせ（Ｓ２２）、広域ＩＰ網ポリシーに違反していないか判断する（Ｓ２３）。

【００２９】ここで、違反していた場合はエントリを中止し、ポリシー受付部１１を介してＶＰＮ管理者にその旨を通知する（Ｓ３０）。許可され、さらにエントリ登録されたＶＰＮポリシーがＶＰＮグループ内でのＶＰＮ間通信に関するものであると判断された場合（Ｓ２４，Ｓ２５）は通信相手先ＶＰＮポリシーの自動生成を行う（Ｓ２６）。この際、双方のＶＰＮが異なるアドレス体系を用いている場合は、ポリシーに記述されたアドレスの変換も同時に行う。

【００３０】さらに通信相手先ＶＰＮのＶＰＮポリシー及び広域ＩＰ網ポリシーに照らし合わせ（Ｓ２６）、許可されれば（Ｓ２７）、ポリシー格納部１３にＶＰＮポリシーを格納し（Ｓ２９）、拒否されればエントリを中止し、ポリシー受付部１１を介してＶＰＮ管理者に結果を通知する（Ｓ３０）。

【００３１】なお、同一ＶＰＮグループ内でないＶＰＮ間通信と判断された場合（Ｓ２４，Ｓ２５）は、自ＶＰＮのＶＰＮポリシーのみをポリシー格納部１３に格納する（Ｓ２９）。

【００３２】エンドユーザがＶＰＮポリシーサービスを享受しようと欲した場合、エンドユーザは利用要求をＰＭＳ１０のポリシー受付部１１に送る（Ｓ４１）。ＰＭＳ１０は、まずポリシー検証機能部１２にてエンドユーザが所属するＶＰＮのＶＰＮポリシーと利用要求の照合を行い（Ｓ４２）、許可判断を行う（Ｓ４３）。不許可の場合、その旨をポリシー受付部１１を介してエンドユーザに通知して処理を終わる（Ｓ４９）。許可された場合、その利用要求がＶＰＮを跨るかどうかの判断を行う（Ｓ４４）。

【００３３】跨っていなければＱｏＳ・セキュリティ制御を行う（Ｓ４８）。跨っていた場合、さらに要求がＶＰＮグループを跨るかどうかの判断を行い（Ｓ４５）、跨っていれば相手先ＶＰＮポリシーとの照合を行い（Ｓ４６）、許可判断を行う（Ｓ４７）。許可判断がされればＱｏＳ・セキュリティ制御を行い（Ｓ４８）、結果通知を行う（Ｓ４９）。

【００３４】また、図１１は前述したＱｏＳ・セキュリティ制御に関する詳細フローチャートを示すものである。

【００３５】前述したステップＳ４８で発出されたＱｏＳ・セキュリティ制御要求は共通プラットフォーム部１４にてＱｏＳ及びセキュリティ成分に分解され（Ｓ５１）、セキュリティ成分をセキュリティ制御装置６の設定情報に変換する（Ｓ５２）。さらに、その設定情報が既にセキュリティ制御装置６に登録されている内容かどうかを判断し（Ｓ５３）、未設定ならばセキュリティポリシー制御部１６を介してセキュリティ制御装置６に設定する（Ｓ５４）。

【００３６】また、ＱｏＳ成分をＱｏＳ制御装置５の設定情報に変換し（Ｓ５５）、ＱｏＳポリシー制御部１５を介してＱｏＳ制御装置５に設定する（Ｓ５６）。設定結果はポリシー受付部１１を介してユーザに通知される（Ｓ５７）。

【００３７】図１２に登録されたＶＰＮポリシーの閲覧画面の一例を、図１３にエンドユーザからのサービス要

求の設定画面の一例を示す。

【００３８】

【発明の効果】以上説明したように、本発明によれば、以下のような優れた効果を奏することができる。

（１）複数ユーザでリソースを共有する広域ＩＰ網上で、各々のＶＰＮの管理者のポリシーに基づいたセキュリティの高いＶＰＮ間通信を行うことが可能となる。

（２）ＶＰＮポリシーを階層的に管理することにより、ＶＰＮ管理者は管理下にあるＶＰＮのポリシーを柔軟に設定変更することが可能となり、ＶＰＮ網管理者及び広域ＩＰ網管理者の稼動が軽減される。さらに、複数のＶＰＮをグループ化し、仮想的な１つのＶＰＮのように見せることでＶＰＮ間のアドレス空間の相違やフィルタリング設定等を意識することなく、一人のＶＰＮ管理者がＶＰＮ間通信のＶＰＮポリシーを簡易に設定することが可能となる。

（３）ＶＰＮを跨るサービス要求に対し、ＱｏＳ制御に連動したＶＰＮ間接続等のセキュリティ制御を自動的に行う等、異なるサービスを制御するエレメントの制御装置を連携制御することにより、設定稼動の軽減と矛盾のない設定が可能となる。

【図面の簡単な説明】

【図１】従来のサービス変更の流れの概略を示すフローチャート

【図２】本発明の実施の形態の一例を示すネットワーク構成図

【図３】ＩＥＴＦ　ｐｏｌｉｃｙ　ＷＧの提案におけるＮＷポリシーの構成情報を示す説明図

【図４】本発明による階層化されたＶＰＮポリシー管理者と管理内容を示す説明図

【図５】ＶＰＮを跨ったサービス要求に対する検証のようすを示す説明図

【図６】本発明のＶＰＮポリシー管理装置の機能ブロック図

【図７】本発明によるサービス変更に関わるやり取りの概略を示す説明図

【図８】広域ＩＰ網ポリシー登録時のフローチャート

【図９】ＶＰＮポリシー登録時のフローチャート

【図１０】ユーザ要求発生時のフローチャート

【図１１】ＱｏＳ・セキュリティ制御に関する詳細フローチャート

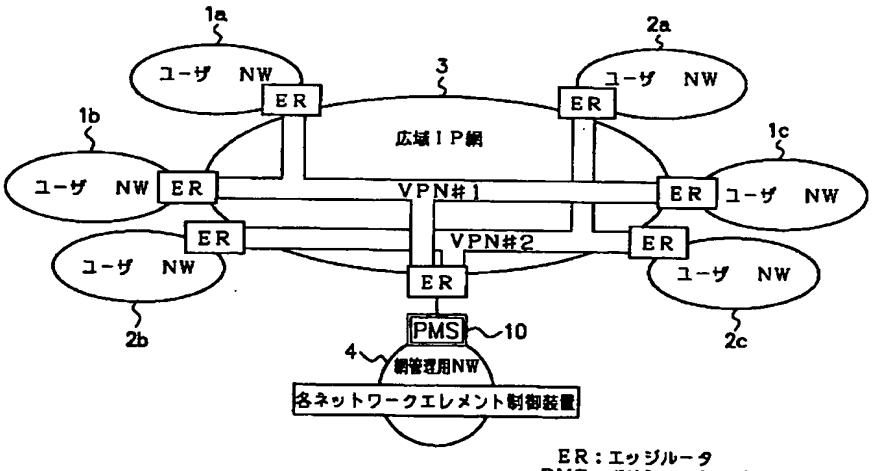
【図１２】ＶＰＮポリシーの閲覧画面の一例を示す図

【図１３】サービス要求の設定画面の一例を示す図

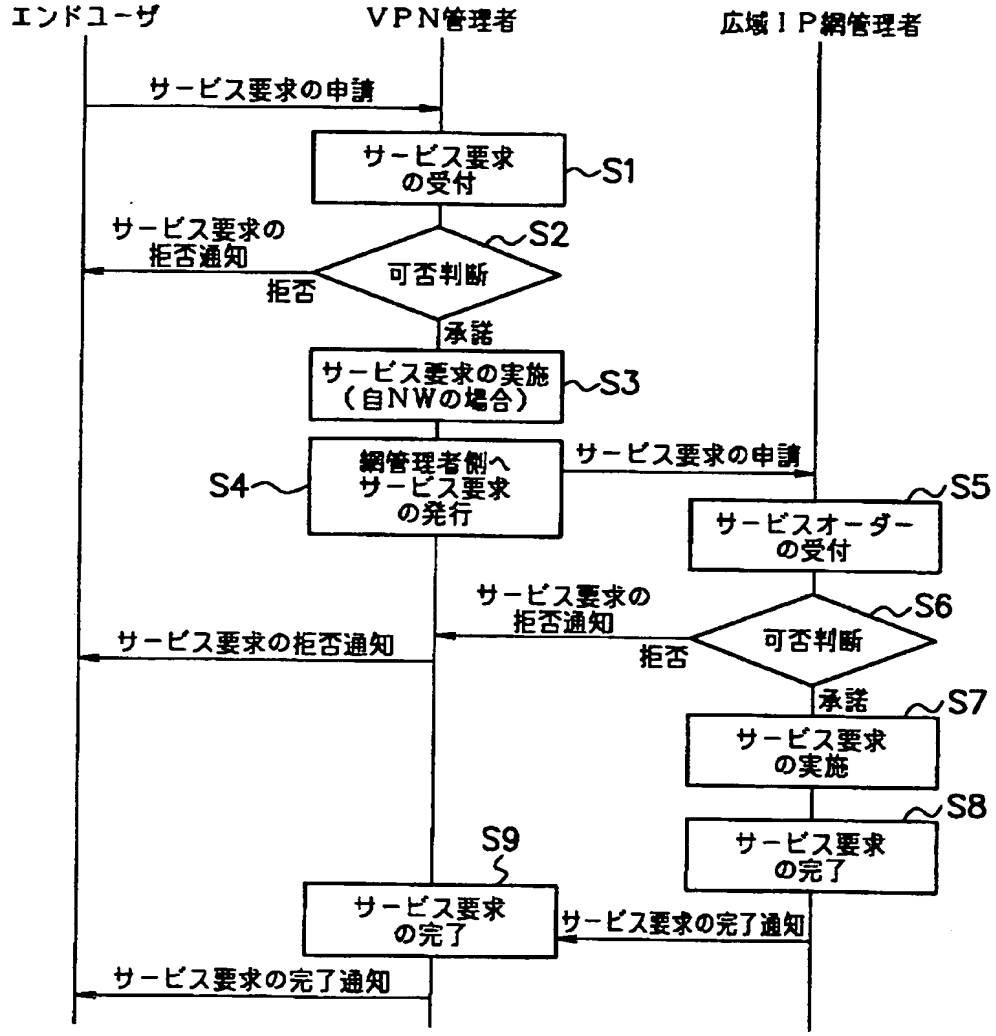
【符号の説明】

１ａ，１ｂ，１ｃ，２ａ，２ｂ，２ｃ：ユーザ、３：広域ＩＰ網、４：網管理用ＮＷ、５：ＱｏＳ制御装置、６：セキュリティ制御装置、１０：ＶＰＮポリシー管理装置、１１：ポリシー受付部、１２：ポリシー検証機能部、１３：ポリシー格納部、１４：共通プラットフォーム部、１５：ＱｏＳポリシー制御部、１６：セキュリティポリシー制御部。

【図２】



【図1】



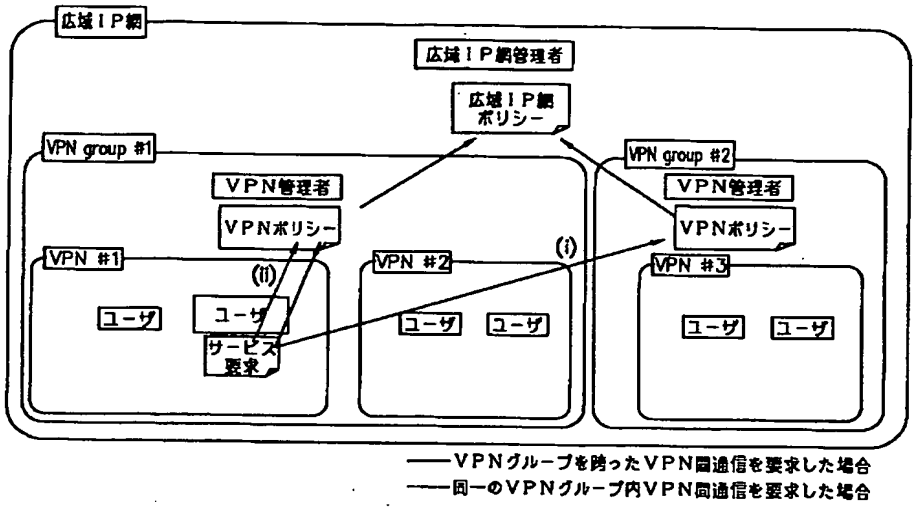
【図3】

構成情報名	構成情報内容
Policy Condition	送信側/受信側のIPアドレスやポート番号，プロトコルなど，制御の対象となるフローの情報を記述
Policy Action	割当てるQoS（優先度や帯域など）や通信の可否など，そのフローに対して行う制御内容を記述
Policy Time Period Condition	Policy Actionが適用される時間帯情報

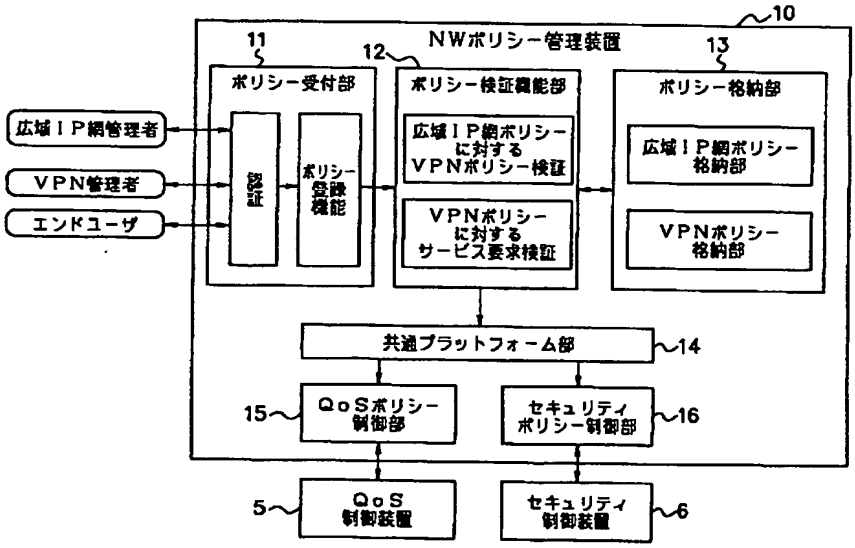
【図4】

管理者名	管理内容	
広域IP網管理者	広域IP網ポリシー：各VPN契約情報	
	Policy Condition	VPNで定義されたアドレス空間
	Policy Action	契約QoSクラス，契約帯域
	Policy Time Period Condition	契約利用時間帯など
VPN管理者	VPNポリシー：管理下にある1または複数のVPN内の帯域，セキュリティなどの利用規定	
	Policy Condition	送信，受信ネットワークアドレス，アプリケーション
	Policy Action	利用可能QoSクラス，利用可能帯域
	Policy Time Period Condition	利用可能時間帯
エンドユーザ	利用ポリシー：エンドユーザからのサービス利用要求	
	Policy Condition	送信，受信端末アドレス，アプリケーション
	Policy Action	要求QoSクラス，要求帯域
	Policy Time Period Condition	利用希望時間帯

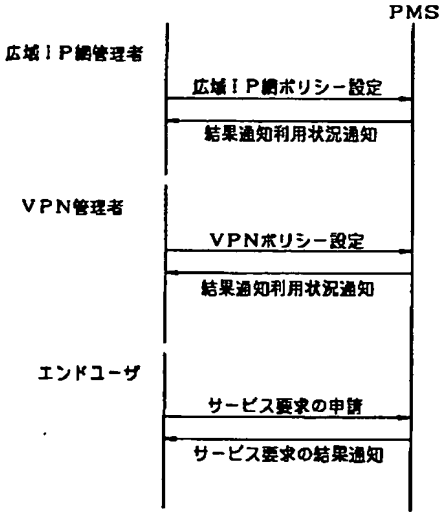
【図5】


広域IP網
広域IP網管理者
広域IP網ポリシー
VPN group #1
VPN group #2
VPN管理者
VPNポリシー
VPN管理者
VPNポリシー
VPN #1
VPN #2
VPN #3
(i)
(ii)
ユーザ
ユーザ
ユーザ
ユーザ
ユーザ
ユーザ
サービス要求
——VPNグループを跨ったVPN間通信を要求した場合
——同一のVPNグループ内VPN間通信を要求した場合

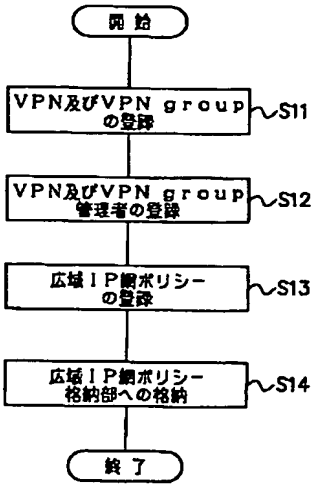
【図6】


10
NWポリシー管理装置
11
12
13
ポリシー受付部
ポリシー検証機能部
ポリシー格納部
広域IP網管理者
VPN管理者
エンドユーザ
認証
ポリシー登録機能
広域IP網ポリシーに対するVPNポリシー検証
VPNポリシーに対するサービス要求検証
広域IP網ポリシー格納部
VPNポリシー格納部
共通プラットフォーム部
14
15
QoSポリシー制御部
セキュリティポリシー制御部
16
5
QoS制御装置
セキュリティ制御装置
6

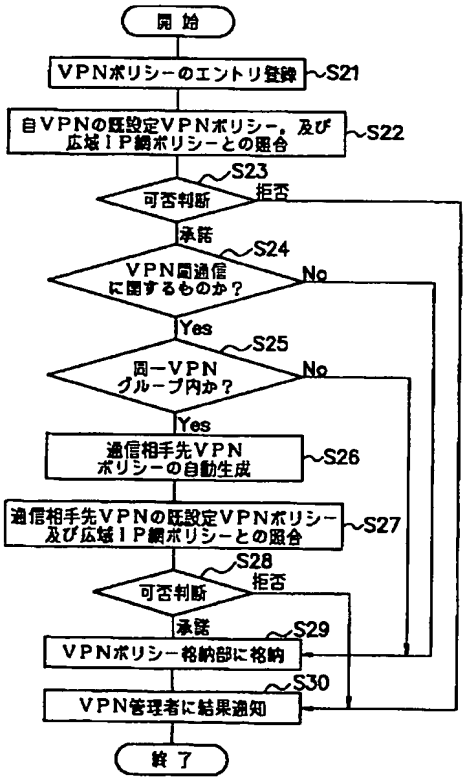
【図7】


PMS
広域IP網管理者
広域IP網ポリシー設定
結果通知利用状況通知
VPN管理者
VPNポリシー設定
結果通知利用状況通知
エンドユーザ
サービス要求の申請
サービス要求の結果通知

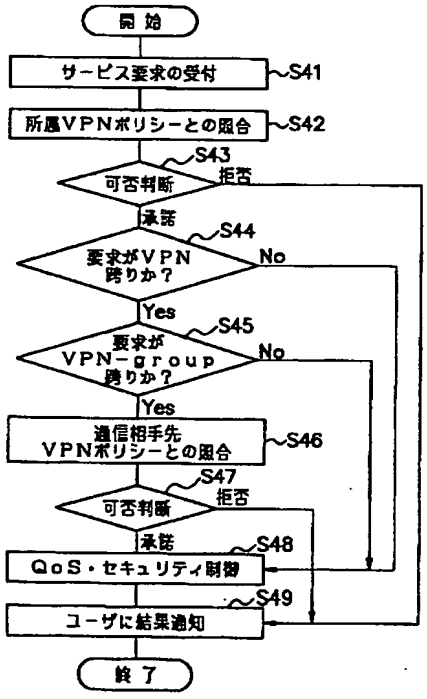
【図8】


開始
VPN及びVPN group の登録
S11
VPN及びVPN group 管理者の登録
S12
広域IP網ポリシー の登録
S13
広域IP網ポリシー 格納部への格納
S14
終了

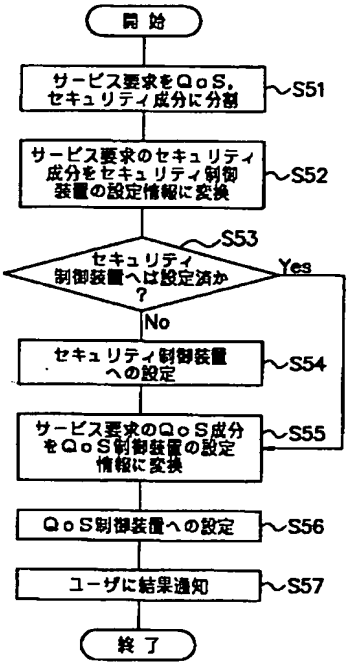
【図9】


開始
VPNポリシーのエントリ登録
S21
自VPNの既設定VPNポリシー、及び 広域IP網ポリシーとの照合
S22
S23
可否判断
拒否
承諾
S24
VPN間通信 に関するものか？
No
Yes
S25
同一VPN グループ内か？
No
Yes
通信相手先VPN ポリシーの自動生成
S26
通信相手先VPNの既設定VPNポリシー 及び広域IP網ポリシーとの照合
S27
S28
可否判断
拒否
承諾
S29
VPNポリシー格納部に格納
S30
VPN管理者に結果通知
終了

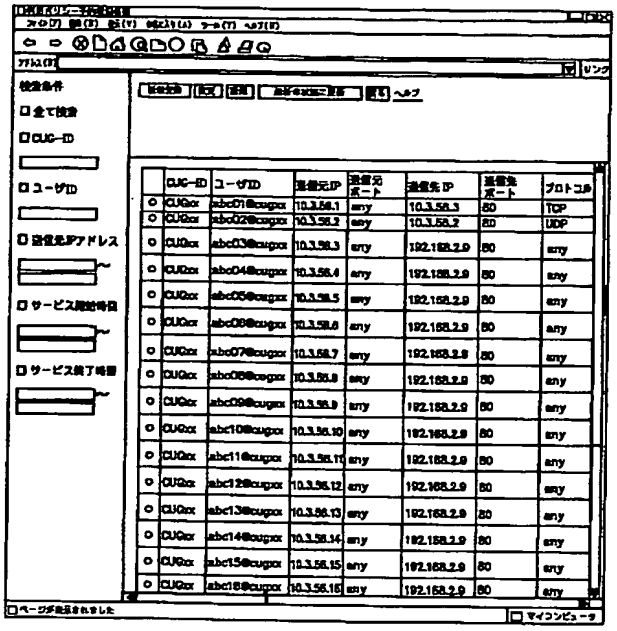
【図10】


開始
サービス要求の受付
S41
所属VPNポリシーとの照合
S42
S43
可否判断
拒否
承諾
S44
要求がVPN 跨りか？
No
Yes
S45
要求が VPN-group 跨りか？
No
Yes
通信相手先 VPNポリシーとの照合
S46
S47
可否判断
拒否
承諾
S48
QoS・セキュリティ制御
S49
ユーザに結果通知
終了

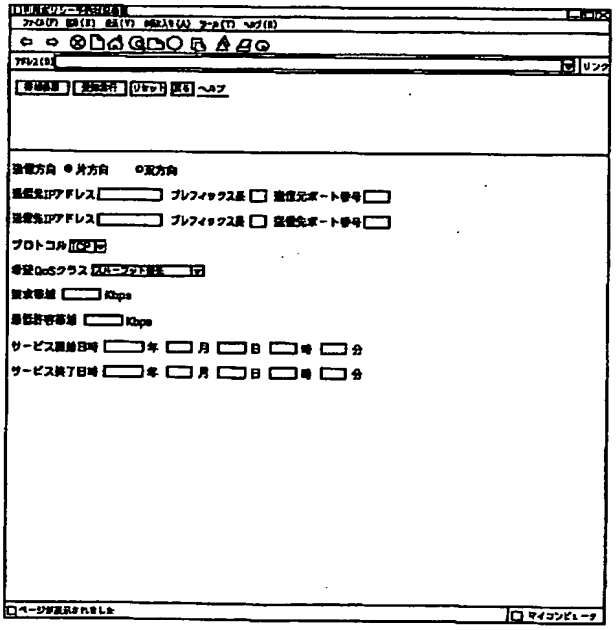
【図１１】


開始
サービス要求をQoS，セキュリティ成分に分割
S51
サービス要求のセキュリティ成分をセキュリティ制御装置の設定情報に変換
S52
S53
セキュリティ制御装置へは設定済か？
Yes
No
セキュリティ制御装置への設定
S54
サービス要求のQoS成分をQoS制御装置の設定情報に変換
S55
QoS制御装置への設定
S56
ユーザに結果通知
S57
終了

【図１２】



【図１３】



(特０))01-251307 (P2001-25でt8

フロントページの続き

(72)発明者　金子　真也
大阪府大阪市中央区馬場町３番15号　西日
本電信電話株式会社内

Fターム(参考)　5K030 GA11 HA08 HC01 HD03 HD07
HD09 JA00 LB20 LC05 LD20
9A001 CC07 KK56 LL09